DOI:
10.1109/TIFS.2018.2848630

Document Version
Peer reviewed version

Energy-Constrained SWIPT Networks: Enhancing Physical Layer Security With FD Self-Jamming

Xuanxuan Tang, Yueming Cai, *Senior Member, IEEE*, Yansha Deng, *Member, IEEE*, Yuzhen Huang, *Member, IEEE*, Wendong Yang, and Weiwei Yang, *Member, IEEE*

***Abstract*—In this paper, we investigate the secrecy performance of energy-constrained wireless powered networks with considering the passive eavesdropping scenario, where the simultaneous wireless information and power transfer based full-duplex self-jamming (SWIPT-FDSJ) scheme is developed. The maximal ratio transmission (MRT) protocol is applied at the multi-antenna source such that the wireless signals are designated to the destination directly. Besides, the energy harvesting and full-duplex (FD) self-jamming operations are adopted at the energy-constrained destination to prolong its lifetime as well as to confuse the eavesdropper. Specifically, the exact and asymptotic closed-form expressions of the connection outage probability (COP), the secrecy outage probability (SOP), and the secrecy throughput of the proposed system are obtained, based on which we optimize the time-switching ratio to maximize the secrecy throughput. We also degenerate the proposed SWIPT-FDSJ scheme to the reduced half-duplex with no self-jamming (HDNSJ) scheme. The finds suggest that in the HDNSJ scheme, adding the antenna number of the source only benefits the COP performance, but has no impact on the SOP performance. By contrast, it will promote the COP and SOP performance at the same time in the SWIPT-FDSJ scheme, which eventually results in the great improvement of secrecy throughput. In addition, we present the practical application condition of the SWIPT-FDSJ scheme. It is demonstrated that the secrecy throughput performance of the SWIPT-FDSJ scheme is much superior to the HDNSJ scheme on condition that the application condition is satisfied.**

***Index Terms*—Energy harvesting, maximum secrecy throughput, secrecy outage probability, time-switching ratio, optimal application condition.**

I. Introduction

DUE to the broadcast nature of the wireless medium, it is important to address the security issue of wireless communication in practical system designs. Traditionally, the security is enhanced by encryption at higher layers [1, 2]. However, with the rapid development of the computing capability, the cryptography-based methods could not ensure the absolute security any longer. Fortunately, the physical layer security technique has emerged recently and is deemed to serve as a good supplement of current cryptographic mechanism. The notion of physical layer security was first proposed by Shannon in 1949 [3] and then significantly promoted by Wyner in 1975 [4]. The basic idea of Wyner is to secure the proposed wiretap channel model by taking advantage of the difference between the physical channels of authorized user and malicious eavesdropper. Since then, enormous researches based on Wyner's notion have been carried out in various networks, like cellular networks [5], cognitive radio (CR) networks [6], wireless sensor networks (WSNs) [7], and a variety of scenarios with single-antenna [8], multi-antenna [9, 10], multiple-input-single-output (MISO) [11] and multiple-input-multiple-output (MIMO) [12, 13], etc.

Practically, the lifetime of wireless devices may be greatly limited by the capacity of their batteries [14]. Except for increasing the battery capacity, there is a strong desire to exploit effective remote charging technologies in some energy-constrained networks like WSNs [15, 16], wireless body area networks (WBANs) [17, 18], etc. Hence, the simultaneous wireless information and power transfer (SWIPT) has recently gained much attention, because it is regarded as a promising technique to transmit both energy and information by the same electromagnetic wave [19]. For example, [20] studied the wireless energy and information transfer trade-off for limited feedback multiantenna systems, where the adaptive energy beamforming was proposed according to the instantaneous channel state information (CSI) for maximizing the harvesting energy. However, the current circuits for wireless energy harvesting can not extract information from the signals [21]. This has triggered extensive study on two prevalent types of energy-harvesting receivers, namely the time-switching (TS) receivers [22, 23] and the power-splitting (PS) receivers [24, 25], where part of the time or power of the received signal is allocated to energy harvesting and the remaining part is used for information processing, respectively.

Recently, the physical layer security of SWIPT networks has received increasing attention [26–28]. In [26], the secrecy performance of a single-input multiple-output (SIMO) SWIPT system was studied, where the base station transmits information to a desired information receiver and at the same time transfers energy to multiple energy-harvesting receivers. Under the assumption that the information may be wiretapped by the energy-harvesting receivers, the authors derived the

This work is supported by the National Natural Science Foundation of China under Grant No. 61771487, 61471393, 61501507, and 61371122, the Jiangsu Provincial Natural Science Foundation of China under Grant No. BK20150719, and the China Scholarship Council. This work is done while X. Tang is a visiting student with the Department of Informatics, King's College London.

X. Tang, Y. Cai, Y. Huang, W. Yang and W. Yang are with the College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China (email: tang_xx@126.com, caiym@vip.sina.com, yzh_huang@sina.com, ywd1110@163.com, wwyang1981@163.com). Y. Huang is also with the Artificial Intelligence Research Center, National Innovation Institute of Defense Technology, Beijing 100166, China, and also with the School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing 100876, China. The corresponding author is Yueming Cai.

Y. Deng is with the Department of Informatics, King's College London, London WC2R 2LS, U.K. (email: yansha.deng@kcl.ac.uk).

closed-form expressions for the secrecy outage probability and the average secrecy capacity, respectively. The authors in [27] proposed a robust secure transmission scheme for MISO SWIPT networks. Taking into account the channel uncertainties, the worst-case secrecy rate was maximized under transmit power constraint and energy-harvesting constraint. An efficient transmission solution for MIMO wiretap channels were presented in [28], where the non-concave problem was firstly converted into a convex optimization, and then was tackled by handling its dual problem.

The physical layer security of SWIPT networks is expected to be further enhanced when jamming operation is exploited [29, 30]. The authors in [31] studied the robust secure transmission with a cooperative jammer helping to confuse the eavesdropper, and the destination harvesting the energy from both the source and the jammer. In [32], the power allocation strategy was investigated to strengthen the security of SWIPT systems with a FD jammer. In this paper, an external jammer is required to be deployed and the energy receiver not only harvests energy but also acts as an eavesdropper.

Other works have looked at the scenarios where additional external jammer is unavailable and the user within the network harvests energy and acts as jammer itself [33–35]. In [33], the secrecy performance of FD SWIPT networks with the PS protocol was studied. A SWIPT transmission system with FD self-jamming was analyzed in [34] in the presence of a passive eavesdropper. In [35], the authors extended the research in the CR networks, where the energy collected by the receiving antenna is used for producing jamming signals. However, [33–35] only considered the single-antenna scenario, which would be not practical any longer when applied to the multi-antenna cases. Moreover, only [34] considered the performance optimization, which was only addressed by numerical simulations, and no exact demonstration for the existence of the optimum point was provided.

In this paper, we propose a new paradigm to strengthen the physical layer security for the energy-constrained SWIPT networks, where the SWIPT based full-duplex (FD) self-jamming (SWIPT-FDSJ) scheme is developed. More specifically, the FD self-jamming is designed to confuse the eavesdropper while the SWIPT is to proposed prolong the lifetime of the energy-constrained destination node[1]. Moreover, the maximal ratio transmission (MRT) protocol is exploited at the source node so that the signals could be designated to the destination node directly. The main contributions are summarized as follows:

- We derive the exact closed-form expressions for the connection outage probability (COP), the secrecy outage probability (SOP), and the secrecy throughput, respectively. The theoretical results can indicate the impacts of the system parameters on the secrecy performance of proposed networks.

[1]We note that, by using the extensively investigated artificial noise at the source is expected to improve the secrecy performance of the network. However, this paper has attempted to explore what effective methods could be taken by a wireless-powered legitimate user to further increase the network security as much as possible even when the eavesdropper's CSI is unknown. The combining of artificial noise and self-jamming operations in the SWIPT networks to mutually promote the secrecy performance would be interesting and will be explored in the future.

TABLE I
LIST OF FUNDAMENTAL VARIABLES

Symbol	Description
N_S	Antenna number of S
T_0	Packet/block time duration
α	Time-switching ratio
$h_{a,b}$	Channel coefficient between a and b
$\bar{\gamma}_{a,b}$	Average channel power gain of $h_{a,b}$
$\mathbf{h}_{a,b}$	Channel coefficient vector between a and b
h_I	Self-interference channel coefficient
$\bar{\gamma}_I$	Average channel power gain of h_I
$\tilde{h}_I$	Self-interference channel coefficient after SIC
$\bar{\tilde{\gamma}}_I$	Average channel power gain of $\tilde{h}_I$
θ	Amount of SIC in dB
$d_{a,b}$	Distance between a and b
μ	Path loss factor
P_S	Transmit power of S
P_J	Transmit power of jamming signal
N_0	Variance of AWGN
η	Energy conversion efficiency
ω	$\omega = \alpha/(1-\alpha)$
R_t	Transmit rate per channel use
R_s	Secrecy rate per channel use
γ_{th}^t	Predefined threshold $\gamma_{th}^t = 2^{R_t} - 1$
γ_{th}^e	Predefined threshold $\gamma_{th}^e = 2^{R_t - R_s} - 1$
P_{CO}	Connection outage probability
P_{SO}	Secrecy outage probability
ς	Secrecy throughput

- As the transmit signal-to-noise ratio (SNR) and the self-interference cancellation (SIC) goes to infinity, we derive the asymptotic expressions of the COP, the SOP, and the secrecy throughput. Moreover, the asymptotic analytical results are validated by the simulations.
- As the self-interference cancellation (SIC) goes to infinity, we further discuss the problem of time allocation optimization, and then obtain the optimal time-switching ratio. We point out that with the given application condition satisfied, the secrecy throughput performance of the proposed scheme is superior to the reduced half-duplex with no self-jamming (HDNSJ) scheme.

The remainder of the work is organized as follows: Section II describes the system model and presents the secure transmission scheme. Section III presents the exact secrecy analysis of the proposed scheme. In section IV, the asymptotic analysis under two different scenarios are carried out. Section V investigates the issue of optimal time switching ratio. Simulation results are provided in Section VI, and Section VII summarizes the contributions of this paper.

Notation: Throughout this paper, the boldface uppercase letters are used to denote matrices or vectors. $(\cdot)^H$ is denoted as the conjugate transpose operation. $F_\gamma(\cdot)$ and $f_\gamma(\cdot)$ represent the cumulative distribution function (CDF) and the probability density function (PDF) of random variable γ, respectively. $\mathbb{E}[\cdot]$ denotes the expectation operation. A list of the fundamental variables is provided in Table I.

II. SYSTEM MODEL

A. System Description

We consider the secrecy performance of the network as depicted in Fig. 1, which consists of a source S, a destination

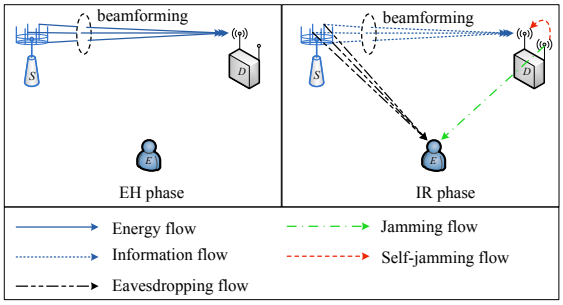


Fig. 1. System Model

D, and a potential eavesdropper E. S is equipped with N_S antennas, D and E are both deployed with a single receiving antenna. Specifically, D is equipped with an extra transmitting antenna to enable the FD operation[2]. We assume that S knows the channel state information (CSI) of D, but has no knowledge about the CSI of E. This is a typical passive eavesdropping scenario, where the malicious eavesdropper may be totally concealed thus it does not feedback its CSI to the source [12, 38]. We assume that all the channels undergo quasi-static Rayleigh fading, such that the channel coefficients keep constant during a packet time T_0 but vary independently from one packet time to another.

B. Secure Transmission: SWIPT and FD Self-Jamming

The SWIPT and FD self-jamming scheme is proposed for safeguarding the data transmission. In more detail, we apply the time-switching SWIPT technology at the destination to extend its battery lifetime [22], where each block time T_0 is split into two phases, namely, the energy harvesting (EH) phase with time period αT_0 and the information receiving (IR) phase with time period $(1-\alpha)T_0$, and $\alpha \in [0,1]$ is the time-switching ratio.

In the EH phase, S transmits the energy-bearing signals to D using maximal ratio transmission (MRT)[3] to increase the harvested energy. Thus, the received signal at D in EH phase is expressed as

$$y_D^{EH} = \sqrt{P_S}\mathbf{h}_{SD}\left(\mathbf{w}_{SD}x_1\right) + n_D, \tag{1}$$

where P_S is the transmit power of S, $\mathbf{h}_{SD} \in \mathbb{C}^{1\times N_S}$ represents the channel coefficient vector between S and D, with its element $h_{S_iD} \sim \mathcal{CN}(0, \sqrt{\bar{\gamma}_{SD}})$[4], $\mathbf{w}_{SD} = (\mathbf{h}_{SD})^H/\|\mathbf{h}_{SD}\|$ is the weight vector of MRT, x_1 denotes the energy-bearing signal with $\mathbb{E}\left[|x_1|^2\right] = 1$, and n_D represents the additive white Gaussian noise (AWGN) at D with zero mean and variance N_0. Hence, the collected energy at D during EH phase can be written as[5]

$$\varepsilon_D = \eta\alpha T_0 P_S |\mathbf{h}_{SD}\mathbf{w}_{SD}|^2, \tag{2}$$

where η denotes the energy conversion efficiency.

In the IR phase, the information-bearing signals are transmitted from S to D, which may be intercepted by E. Meanwhile D sends jamming signals using its transmit antenna to confuse the eavesdropper. We note that the MRT scheme is still applied at S in this stage to maximize the receiving SNR at D. As the CSI of E is totally unknown at the legitimate network, such operation as well as the self-jamming in fact attempts to guarantee the best secrecy performance in the data transmission. As a result, the received signals at D and E in IR phase are given by

$$y_D^{IR} = \sqrt{P_S}\mathbf{h}_{SD}\left(\mathbf{w}_{SD}x_2\right) + \sqrt{P_J}h_I x_0 + n_D, \tag{3}$$

and

$$y_E^{IR} = \sqrt{P_S}\mathbf{h}_{SE}\left(\mathbf{w}_{SD}x_2\right) + \sqrt{P_J}h_{DE}x_0 + n_E, \tag{4}$$

where P_J is the jamming power of D, $\mathbf{h}_{SE} \in \mathbb{C}^{1\times N_S}$ denotes the channel vector between S and E, with its element $h_{S_iE} \sim \mathcal{CN}(0, \sqrt{\bar{\gamma}_{SE}})$ and $i \in \{1, 2, \cdots, N_S\}$. In (3) and (4), x_2 and x_0 are the information-bearing signal and the jamming signal with $\mathbb{E}\left[|x_2|^2\right] = \mathbb{E}\left[|x_0|^2\right] = 1$, h_I is the self-interference channel at D with $\mathbb{E}\left[|h_I|^2\right] = \bar{\gamma}_I$, $h_{DE} \sim \mathcal{CN}(0, \sqrt{\bar{\gamma}_{DE}})$ represents the channel between D and E, n_E represents the additive white Gaussian noise (AWGN) at E with zero mean and variance N_0[6].

We assume that the SIC is applied at the FD node D [23, 25, 45]. The receiving signal-to-interference-plus-noise ratios (SINRs) at D and E are calculated as

$$\gamma_D = \frac{P_S|\mathbf{h}_{SD}\mathbf{w}_{SD}|^2}{P_J\left|\tilde{h}_I\right|^2 + N_0}, \tag{5}$$

and

$$\gamma_E = \frac{P_S|\mathbf{h}_{SE}\mathbf{w}_{SD}|^2}{P_J|h_{DE}|^2 + N_0}, \tag{6}$$

where $\tilde{h}_I$ is the self-interference channel after SIC. According to [23, 25], $\tilde{h}_I$ can be treated as a complex Gaussian random variable with $\tilde{h}_I \sim \mathcal{CN}\left(0, \sqrt{\tilde{\bar{\gamma}}_I}\right)$, where $[\tilde{\bar{\gamma}}_I]_{\mathrm{dB}} = [\bar{\gamma}_I]_{\mathrm{dB}} - \theta$, and θ is the amount of SIC in dB. As can be seen from (5)-(6), the jamming operation plays a dual role in the proposed scheme, similar as in [46, 47]. On the one hand, the jamming degenerates the receiving performance of the eavesdropper. On the other hand, a portion of time duration must be sacrificed for collecting energy consumed by sending jamming signals.

Furthermore, as described previously, D is an energy-constrained equipment. Thereby, the jamming power must be chosen to keep the energy balanced at D statistically in

[2]Similar FD deployment has been adopted in numerous works [36, 37].

[3]The CSI for MRT may be imperfect, which will degrade the effect of MRT operation. The imperfect CSI has been extensively investigated by introducing the channel estimation error variable in the channel modeling [39–41], which will be treated in future works.

[4]We note that the large-scale path loss is modeled as $\mathbb{E}\left[\bar{\gamma}_{a,b}\right] = d_{a,b}^{-\mu}$, where $d_{a,b}$ is the distance of link $a-b$, μ represents the path loss factor [6, 7, 42].

[5]We note that little energy can be harvested from the AWGN in practice, hence is neglected in this paper [23, 24].

[6]Without any loss of generality, the variance of AWGN at all receivers within the network is set to be the same [43, 44].

the long run[7]. Practically, we choose P_J according to the following expression [25]

$$P_J = \frac{\mathbb{E}\left[\varepsilon_D\right]}{(1-\alpha)\,T_0} = \omega\eta P_S \mathbb{E}\left[\left|\mathbf{h}_{SD}\mathbf{w}_{SD}\right|^2\right], \tag{7}$$

where $\omega = \alpha/(1-\alpha)$. According to [49], $\left\|\mathbf{h}_{SD}\mathbf{w}_{SD}\right\|^2 = \sum_{i=1}^{N_S}\left|h_{S_iD}\right|^2$ conforms to Erlang distribution with the expectation $N_S\bar{\gamma}_{SD}$. Therefore, the above expression can be rewritten as

$$P_J = \omega\eta N_S\bar{\gamma}_{SD}P_S. \tag{8}$$

III. Exact Performance Analysis

In this section, we study the reliability and security performance of the SWIPT and FD self-jamming scheme by deriving the exact expressions of COP, SOP, and secrecy throughput, respectively.

A. COP and SOP

The COP is defined as the probability of the connection outage event that the receiving SINR at the legitimate receiver falls below a predefined threshold γ_{th}^t, where $\gamma_{th}^t = 2^{R_t} - 1$ and $R_t\,(bits/s/Hz)$ is the transmit rate per channel use[8]. Mathematically, the COP can be calculated as [6, 51]

$$P_{CO} = \Pr\left(\gamma_D < \gamma_{th}^t\right) = F_{\gamma_D}\left(\gamma_{th}^t\right). \tag{9}$$

Lemma 1: The COP of the SWIPT and FD self-jamming system is given by

$$P_{CO} = 1 - \frac{N_0}{\omega\eta N_S\bar{\gamma}_{SD}P_S\tilde{\bar{\gamma}}_I}\sum_{n=0}^{N_S-1}\frac{1}{n!}\left(\frac{N_0\gamma_{th}^t}{P_S\bar{\gamma}_{SD}}\right)^n e^{-\frac{N_0\gamma_{th}^t}{P_S\bar{\gamma}_{SD}}} \times \sum_{n_1=0}^{n}\binom{n}{n_1}(n_1)!\left(\frac{P_S\bar{\gamma}_{SD}\omega\eta N_S\tilde{\bar{\gamma}}_I}{\omega\eta N_S\tilde{\bar{\gamma}}_I N_0\gamma_{th}^t + N_0}\right)^{n_1+1}. \tag{10}$$

Proof: See Appendix A. ∎

The SOP is defined as the probability of the secrecy outage event that the receiving SINR at the eavesdropper is higher than a predefined threshold γ_{th}^e, where $\gamma_{th}^e = 2^{R_t - R_s} - 1$ and $R_s\,(bits/s/Hz)$ is the secrecy rate per channel use. Mathematically, the SOP is defined as [6, 51]

$$P_{SO} = \Pr\left(\gamma_E \geq \gamma_{th}^e\right) = 1 - F_{\gamma_E}\left(\gamma_{th}^e\right). \tag{11}$$

Lemma 2: The SOP of the SWIPT and FD self-jamming system is given by

$$P_{SO} = \frac{\bar{\gamma}_{SE}}{\omega\eta N_S\bar{\gamma}_{SD}\bar{\gamma}_{DE}\gamma_{th}^e + \bar{\gamma}_{SE}}e^{-\frac{N_0\gamma_{th}^e}{P_S\bar{\gamma}_{SE}}}. \tag{12}$$

Proof: See Appendix B. ∎

[7]We note that the energy consumption required by the transmit/receive circuits at the receiver is negligible in this study [21, 38, 48].

[8]The design of R_t and the following R_s falls into the construction of the wiretap coding, which has been elaborated abundantly in the literatures [4, 6, 50], thus is omitted in this paper.

B. Secrecy Throughput Analysis

In the passive eavesdropping scenario, the CSI of E cannot be derived by the legitimate network and the perfect secrecy is not guaranteed. As a consequence, the metric of secrecy throughput becomes appealing which quantifies the average rate of the messages that are reliably and securely transmitted. Mathematically, the secrecy throughput is defined as the equivalent secrecy rate multiplied by the probability of a reliable and secure transmission, which can be written as [6, 51]

$$\varsigma = (1-\alpha)\,R_s P_{R\,\&\,S}, \tag{13}$$

where the term $(1-\alpha)$ results from the time-switching protocol at D, and $P_{R\&S}$ is defined as

$$P_{R\,\&\,S} = \Pr\left(\gamma_D \geq \gamma_{th}^t, \gamma_E < \gamma_{th}^e\right). \tag{14}$$

Theorem 1: The secrecy throughput for the SWIPT and FD self-jamming system is given by

$$\varsigma = \frac{R_s}{1+\omega}\left(1 - \frac{\bar{\gamma}_{SE}}{\omega\eta N_S\bar{\gamma}_{SD}\bar{\gamma}_{DE}\gamma_{th}^e + \bar{\gamma}_{SE}}e^{-\frac{N_0\gamma_{th}^e}{P_S\bar{\gamma}_{SE}}}\right) \times \frac{N_0}{\omega\eta N_S\bar{\gamma}_{SD}P_S\tilde{\bar{\gamma}}_I}\sum_{n=0}^{N_S-1}\frac{1}{n!}\left(\frac{N_0\gamma_{th}^t}{P_S\bar{\gamma}_{SD}}\right)^n e^{-\frac{N_0\gamma_{th}^t}{P_S\bar{\gamma}_{SD}}} \times \sum_{n_1=0}^{n}\binom{n}{n_1}(n_1)!\left(\frac{P_S\bar{\gamma}_{SD}\omega\eta N_S\tilde{\bar{\gamma}}_I}{\omega\eta N_S\tilde{\bar{\gamma}}_I N_0\gamma_{th}^t + N_0}\right)^{n_1+1}, \tag{15}$$

where $\omega = \alpha/(1-\alpha)$.

Proof: As has been described, $\mathbf{w}_{SD} = [w_1, \cdots w_n, \cdots w_{N_S}]^T$ is a normalized vector, i.e., $\sum_{n=1}^{N_S}\left|w_n\right|^2 = 1$. Thus, $|\mathbf{h}_{SE}\mathbf{w}_{SD}|$ is a unitary transformation of $\mathbf{h}_{SE}$. Besides, it is obviously that $\mathbf{w}_{SD}$ is independent of $\mathbf{h}_{SE}$. Moreover, the elements of $\mathbf{h}_{SE}$ are all Gaussian variables, namely $h_{S_nE} \sim \mathcal{N}(0, \bar{\gamma}_{SE})$ for $n \in \{1, 2, \cdots, N_S\}$. Therefore, we can conclude that $w_n h_{S_nE} \sim \mathcal{N}\left(0, |w_n|^2\bar{\gamma}_{SE}\right)$. Hence, $\sum_{n=1}^{N_S} w_n h_{S_nE} \sim \mathcal{N}\left(0, \sum_{n=1}^{N_S}|w_n|^2\bar{\gamma}_{SE}\right) = \mathcal{N}(0, \bar{\gamma}_{SE})$, which verifies that the unitary transformation does not change the distribution of the transformed variables in $\mathbf{h}_{SE}$. As such, the common term of $\mathbf{w}_{SD}$ will not result in any correlation between $|\mathbf{h}_{SD}\mathbf{w}_{SD}|$ and $|\mathbf{h}_{SE}\mathbf{w}_{SD}|$. Therefore, γ_D and γ_E are independent variables [38, 55, 56]. Hence, (14) can be written as

$$P_{R\&S} = \left[1 - P_{CO}\left(\gamma_{th}^t\right)\right]\left[1 - P_{SO}\left(\gamma_{th}^e\right)\right]. \tag{16}$$

By substituting (10) and (12) into (16) and (13) yields the result in Theorem 1. ∎

Theorem 1 provides an analytical expression for the secrecy throughput of the system, which is in closed-form and does not involve any special functions. As a result, it allows for fast evaluation in popular mathematical software such as Matlab, thereby providing an efficient way to access the secrecy throughput of the system while avoiding the time-consuming Monte Carlo simulations.

IV. Asymptotic Performance Analysis

To further exploit the insights from the secrecy performance, the asymptotic analysis is conducted under two scenarios, namely: (A) the scenario with high transmit SNR[9], i.e., $\gamma_S \to \infty$; and (B) the scenario with large amount of SIC, i.e., $\theta \to \infty$[10].

A. The Scenario with $\gamma_S \to \infty$.

Lemma 3: The COP for the SWIPT and FD self-jamming system with $\gamma_S \to \infty$ is derived as

$$P_{CO}^{\gamma_S\to\infty} = 1 - \frac{1}{\omega\eta N_S \bar{\gamma}_{SD}\tilde{\bar{\gamma}}_I} \sum_{n=0}^{N_S-1} \left(\frac{\gamma_{th}^t}{\bar{\gamma}_{SD}}\right)^n \times \left(\frac{\omega\eta N_S \tilde{\bar{\gamma}}_I \bar{\gamma}_{SD}}{\omega\eta N_S \tilde{\bar{\gamma}}_I \gamma_{th}^t + 1}\right)^{n+1}. \quad (17)$$

Proof: For $\gamma_S \to \infty$, we have

$$\gamma_D^{\gamma_S\to\infty} = \frac{|\mathbf{h}_{SD}\mathbf{w}_{SD}|^2}{\omega\eta N_S \bar{\gamma}_{SD}\left|\tilde{h}_I\right|^2}. \quad (18)$$

As (18) is similar to (5), hence (17) can be easily obtained by following a similar proof as in Lemma 1. ∎

Lemma 4: The SOP for the SWIPT and FD self-jamming system with $\gamma_S \to \infty$ is given by

$$P_{SO}^{\gamma_S\to\infty} = \frac{\bar{\gamma}_{SE}}{\omega\eta N_S \bar{\gamma}_{SD}\bar{\gamma}_{DE}\gamma_{th}^e + \bar{\gamma}_{SE}}. \quad (19)$$

Proof: Under the scenario of $\gamma_S \to \infty$, we have

$$\gamma_E^{\gamma_S\to\infty} = \frac{|\mathbf{h}_{SE}\mathbf{w}_{SD}|^2}{\omega\eta N_S \bar{\gamma}_{SD}|h_{DE}|^2}. \quad (20)$$

Following the similar proof as in Lemma 2, (20) is readily derived. ∎

Armed with the results in Lemmas 3 and 4, we proceed to investigate the corresponding secrecy throughput performance.

Theorem 2: The secrecy throughput for the SWIPT and FD self-jamming system with $\gamma_S \to \infty$ is given by

$$\varsigma^{\gamma_S\to\infty} = \frac{R_s}{1+\omega} \sum_{n=0}^{N_S-1} \left(\frac{\gamma_{th}^t}{\bar{\gamma}_{SD}}\right)^n \left(\frac{\omega\eta N_S \tilde{\bar{\gamma}}_I \bar{\gamma}_{SD}}{\omega\eta N_S \tilde{\bar{\gamma}}_I \gamma_{th}^t + 1}\right)^{n+1} \times \frac{1}{\omega\eta N_S \bar{\gamma}_{SD}\tilde{\bar{\gamma}}_I}\left(1 - \frac{\bar{\gamma}_{SE}}{\omega\eta N_S \bar{\gamma}_{SD}\bar{\gamma}_{DE}\gamma_{th}^e + \bar{\gamma}_{SE}}\right). \quad (21)$$

Proof: By substituting (17) and (19) into (16) and (13) easily yields the result in Theorem 2. ∎

It is worth noting that Theorem 2 presents general closed-form expressions of the asymptotic secrecy throughput which remains sufficiently tight when $\gamma_S \to \infty$ as will be demonstrated in Section VI. Hence, this new analytical expression provides an efficient way to characterize the impact of key system parameters such as antenna number of the source, distances between the nodes, and the amount of SIC on the secrecy throughput of the system, without resorting to the time-consuming Monte Carlo simulations.

B. The Scenario with $\theta \to \infty$.

Lemma 5: The SOP for the SWIPT and FD self-jamming system with $\theta \to \infty$ is the same as Eq. (12), while the COP for the SWIPT and FD self-jamming system with $\theta \to \infty$ is given by

$$P_{CO}^{\theta\to\infty} = 1 - \sum_{n=0}^{N_S-1} \frac{1}{n!}\left(\frac{N_0\gamma_{th}^t}{P_S\bar{\gamma}_{SD}}\right)^n e^{-\frac{N_0\gamma_{th}^t}{P_S\bar{\gamma}_{SD}}}. \quad (22)$$

Proof: As can be readily observed, when $\theta \to \infty$, the expression of γ_E remains unchanged. Hence, the SOP under this scenario is the same as Eq. (12). As for the COP, we have

$$\gamma_D^{\theta\to\infty} = \frac{P_S}{N_0}\|\mathbf{h}_{SD}\mathbf{w}_{SD}\|^2. \quad (23)$$

To this end, the result in Eq. (22) could be extracted from (32) by replacing x with γ_{th}^t. ∎

Based on the results in Lemma 5, we carry on studying the corresponding secrecy throughput performance.

Theorem 3: The secrecy throughput for the SWIPT and FD self-jamming system with $\theta \to \infty$ is given by

$$\varsigma^{\theta\to\infty} = \frac{R_s}{1+\omega} \sum_{n=0}^{N_S-1} \frac{1}{n!}\left(\frac{N_0\gamma_{th}^t}{P_S\bar{\gamma}_{SD}}\right)^n e^{-\frac{N_0\gamma_{th}^t}{P_S\bar{\gamma}_{SD}}} \times \left(1 - \frac{\bar{\gamma}_{SE}}{\omega\eta N_S \bar{\gamma}_{SD}\bar{\gamma}_{DE}\gamma_{th}^e + \bar{\gamma}_{SE}} e^{-\frac{N_0\gamma_{th}^e}{P_S\bar{\gamma}_{SE}}}\right). \quad (24)$$

Proof: By substituting (12) and (22) into (16) and (13), we easily proved the result in Theorem 3. ∎

We note that, the FD operation is designed to send self-jamming signals. As a result, when HDNSJ scheme is applied, there will be no need to split any time duration for harvesting energy, which acts as the energy supply for the self-jamming operation in our proposed scheme. Therefore, with $\alpha = 0$ and $\theta \to \infty$, our proposed SWIPT-FDSJ scheme can be easily reduced to HDNSJ scheme. In other words, our proposed scheme is more generalized, and the HD scheme without self-jamming is a special case of our analysis. The reduced expressions of SOP, COP and secrecy throughput for HDNSJ scheme can be easily derived from (12), (22) and (24) by letting $\omega = 0$ (i.e., $\alpha = 0$).

V. Optimal Time Duration Allocation

As mentioned previously, the time-switching ratio α is an important parameter, which directly determines the effect of the jamming protocol. We note that, there exists an optimal α maximizing the system secrecy throughput. On one hand, according to Eq. (8), a larger α indicates a higher jamming power. Hence, the eavesdropper would generally be confused and suppressed greater, thus the secrecy throughput will be improved. On the other hand, a larger α also means the decline of time duration allocated for data transmission, which in turn leads to the decrease of the secrecy throughput. Thereby, it

[9]The transmit SNR is defined as $\gamma_S = P_S/N_0$.

[10]We note that an amount of SIC up to 40 dB would satisfy this requirement in this paper, which can be well supported by current passive SIC methods like directional SIC, antenna separation and SIC, etc. These methods suppress the self-interference by physical separation and thus do not consume any energy [25, 31].

must be carefully designed according to the specific environment to achieve the best secrecy throughput performance.

Mathematically, the optimization problem could be written as

$$\varsigma_{\max} = \arg\max_{\alpha} \varsigma(\alpha), \quad \text{subject to}: \ 0 \le \alpha \le 1. \tag{25}$$

Noting that α is monotonically increased with ω. Therefore, the above problem could be reformulated as

$$\varsigma_{\max} = \arg\max_{\omega} \varsigma(\omega), \quad \text{subject to}: \ 0 \le \omega < \infty. \tag{26}$$

Unfortunately, it is too involved to reveal the monotonicity and convexity in Eq. (14) with respect to ω. In order to make it traceable, we use the asymptotic result with $\theta \to \infty$, namely Eq. (24) instead. As a result, the optimization problem is expressed as

$$\varsigma_{\max} = \arg\max_{\omega} \varsigma^{\theta\to\infty}(\omega), \ \text{subject to}: 0 \le \omega < \infty. \tag{27}$$

***Theorem** 4:* The optimal value of time-switching ratio α and the corresponding maximum secrecy throughput for the SWIPT and FD self-jamming system with $\theta \to \infty$ are given by (28) and (29), respectively

$$\alpha^* = \begin{cases} 0, & \kappa_2 \le \frac{\kappa_1}{1+\kappa_1} \\ \frac{\omega^*}{1+\omega^*}, & \kappa_2 > \frac{\kappa_1}{1+\kappa_1} \end{cases}, \tag{28}$$

$$\varsigma_{\max}^{\theta\to\infty} = g_{\max} R_s \sum_{n=0}^{N_S-1} \frac{1}{n!} \left(\frac{N_0 \gamma_{th}^t}{P_S \bar{\gamma}_{SD}} \right)^n e^{-\frac{N_0 \gamma_{th}^t}{P_S \bar{\gamma}_{SD}}}, \tag{29}$$

where

$$g_{\max} = \begin{cases} (1-\kappa_2), & \kappa_2 \le \frac{\kappa_1}{1+\kappa_1} \\ \frac{1}{1+\omega^*} \left(1 - \frac{\kappa_1 \kappa_2}{\omega^* + \kappa_1} \right), & \kappa_2 > \frac{\kappa_1}{1+\kappa_1} \end{cases}, \tag{30}$$

with

$$\begin{cases} \omega^* = -\kappa_1 (1-\kappa_2) + \sqrt{\kappa_1 \kappa_2 (1 + \kappa_1 \kappa_2 - \kappa_1)} \\ \kappa_1 = \frac{\bar{\gamma}_{SE}}{\eta N_S \bar{\gamma}_{SD} \bar{\gamma}_{DE} \gamma_{th}^e} \\ \kappa_2 = e^{-\frac{\gamma_{th}^e}{\gamma_S \bar{\gamma}_{SE}}} \end{cases}. \tag{31}$$

Proof: See Appendix C. ■

It is highlighted that $\alpha^* = 0$ indicates that no energy is harvested, and thus no jamming signal is exploited. Therefore, $\alpha^* = 0$ actually degenerates to the conventional case with no SWIPT and jamming. In other words, Theorem 4 gives the application condition of the proposed scheme, namely $\kappa_2 > \kappa_1/(1+\kappa_1)$, and at the same time provides the maximum secrecy throughput of it when the condition is satisfied. We note that the application condition is totally determined by the transmit SNR, the antenna number of the source, the energy conversion efficiency, and the average channel gains of both the authorized and malicious links.

TABLE II
LIST OF KEY SIMULATION PARAMETERS

Parameters	Values	Parameters	Values
N_S	2	R_t	3 bits/s/Hz
R_s	2 bits/s/Hz	η	0.6
α	0.5	N_0	1
T_0	1	d_{SD}	1.5 m
d_{SE}	1.5 m	d_{DE}	1.5 m
μ	2.7	θ	40 dB

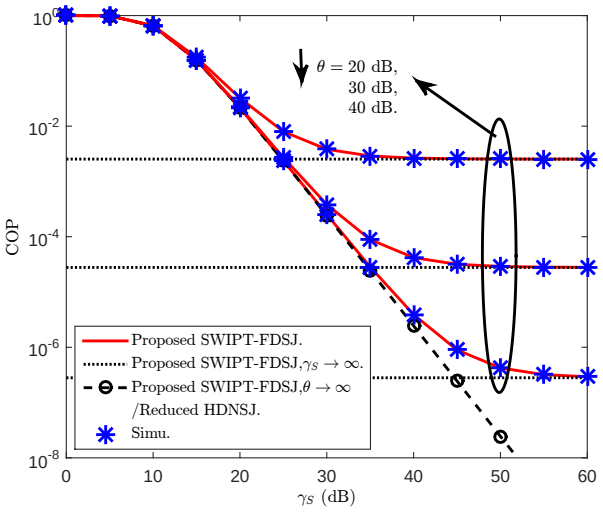


Fig. 2. COP vs. γ_S with different θ under α=0.5, η=0.6, R_t=3, R_s=2, N_S=2.

VI. NUMERICAL RESULTS

In this part, we present the numerical results to demonstrate the impacts of various system parameters on the secure performance of the SWIPT and FD self-jamming system. As it is shown from these figures, the theoretical results are in exact agreement with the numerical simulations, which show the correctness of the analysis. Without any loss of generality, the key simulation parameters are listed in Table II unless otherwise stated.

Figs. 2 and 3 examine the impact of γ_S and θ on the COP of the SWIPT and FD self-jamming system. As depicted in these two figures, the COP first decreases significantly and then reaches a performance floor with increasing γ_S and θ. It is also found from Fig. 2 that the exact COP expression in (10) matches the asymptotic result with $\theta \to \infty$ in (17) very well in the low and medium regime of γ_S, and then deviates it with approaching the other asymptotic expression with $\gamma_S \to \infty$, namely (22), when the transmit SNR is high enough. Generally speaking, a larger amount of SIC is needed to reach the performance floor when a larger transmit SNR is provided. The similar phenomenon is also observed for θ in Fig. 3.

Figs. 4 and 5 illustrate the COP and SOP of the SWIPT and FD self-jamming system with different N_S. As we can see from Fig. 4, the COP is an increasing function of N_S and an obvious performance enhancement is achieved with

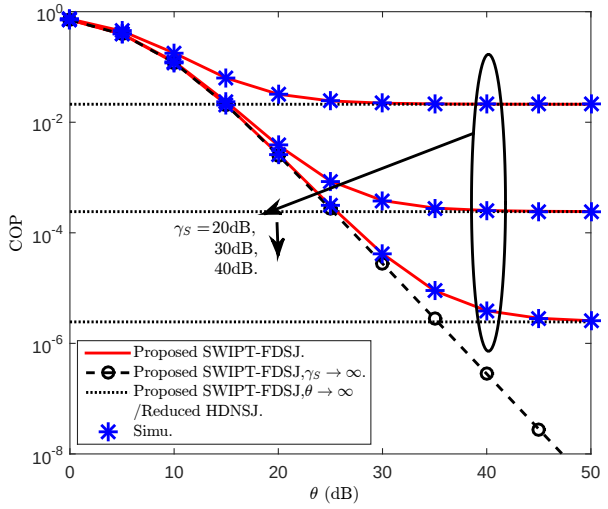


Fig. 3. COP vs. θ with different γ_S under α=0.5, η=0.6, R_t=3, R_s=2, N_S=2.

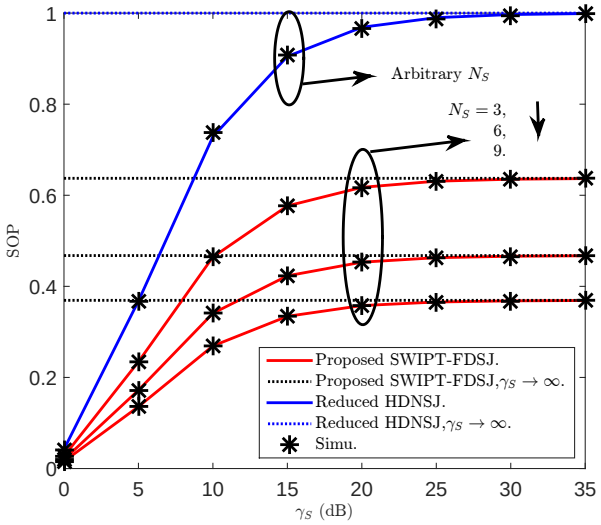


Fig. 5. SOP vs. γ_S with different N_S under α=0.5, η=0.6, R_t=3, R_s=2.

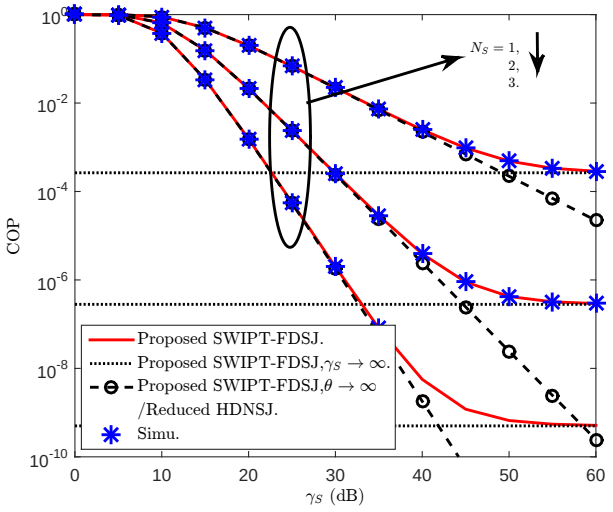


Fig. 4. COP vs. γ_S with different N_S under α=0.5, η=0.6, R_t=3, R_s=2, θ=40 dB.

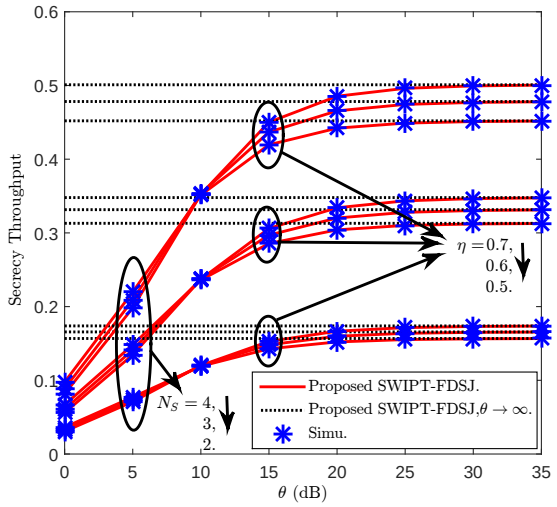


Fig. 6. Secrecy throughput vs. θ with different N_S and η under α=0.5, R_t=3, R_s=2, θ=40 dB.

the increase of N_S. In addition, as in Fig. 2 and 3, Eqs. (17) and (22) provide good approximations of the exact theoretical result in the corresponding cases. On the contrary, we find in Fig. 5 that the SOP goes an inverse trend when comparing with COP. Although an improvement is also found when N_S grows, it is not as distinct as that in COP. It is worth noting that, some meaningful insights are found from Fig. 2-5 when comparing the proposed SWIPT-FDSJ scheme with the reduced HDNSJ scheme. Obviously, the introducing of FD self-jamming has a negative impact on the COP performance, which however becomes very slight with the increase of θ. By contrast, the self-jamming operation has improved the SOP performance significantly, as a distinct performance gap is observed in Fig. 5 between the two group lines (blue and red). Specifically, it is observed that in the HDNSJ scheme, it is useless to decrease the SOP by increasing N_S. We note that, in the considered passive eavesdropping scenario, the legitimate nodes do not have the CSI of the eavesdropper, so that beamforming methods could not be used to interfere it as much as possible. However, in our proposed SWIPT-FDSJ scheme, the SOP performance can be greatly boosted by increasing N_S.

Fig. 6 plots the secrecy throughput of the SWIPT and FD self-jamming system for various N_S and η. As can be observed, the larger N_S and η are, the larger the secrecy throughput is. This is readily understandable, because a larger N_S or η indicates a larger power of jamming signal, so that the eavesdropper is better confused. Furthermore, we see that the secrecy throughput improves significantly with increasing N_S. By contrast, the enhancement with a larger η is almost

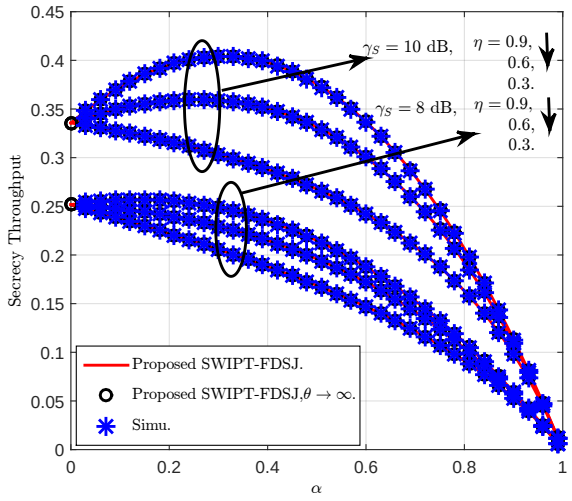


Fig. 7. Secrecy throughput vs. α with different γ_S and η under α=0.5, R_t=3, R_s=2, θ=40 dB, N_S=3.

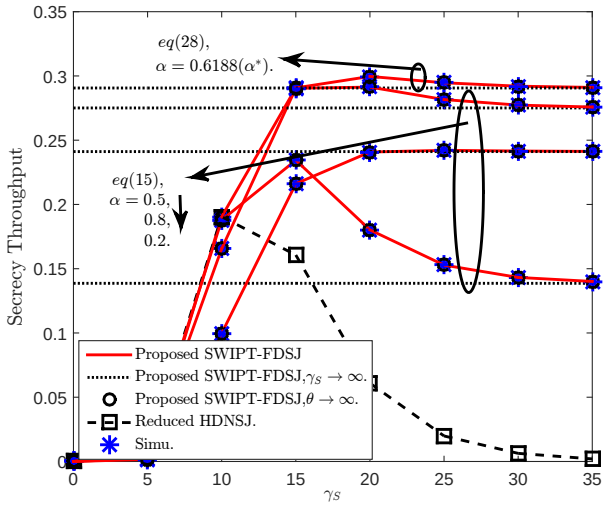


Fig. 8. Secrecy throughput vs. γ_S with different α . R_t=3, R_s=2, θ=40 dB, N_S=2.

ignorable.

TABLE III
VALUE OF $\kappa_2 - \kappa_1/(1+\kappa_1)$ AND α^*

P_S (dB)	η	$\kappa_2 - \kappa_1/(1+\kappa_1)$	α^*
8	0.3	-0.1726	0
	0.6	-0.0315	0
	0.9	0.0664	0.1352
10	0.3	-0.0496	0
	0.6	0.0916	0.2552
	0.9	0.1895	0.3083

Fig. 7 plots the secrecy throughput of the SWIPT and FD self-jamming system for various γ_S and η. In this figure, the optimum condition of secrecy throughput in Theorem 4 is verified by presenting six curves, whose values of $\kappa_2 - \kappa_1/(1+\kappa_1)$ are listed in Table III. As can be expected, three curves corresponding to γ_S=8 dB, η=0.3 and 0.6 and γ_S=10 dB, η=0.3 are monotonically decreasing, which all satisfy the condition of $\kappa_2 - \kappa_1/(1+\kappa_1) \leq 0$. Whereas, the remaining three curves satisfying $\kappa_2 - \kappa_1/(1+\kappa_1) > 0$ all go up at first and then drop with the increase of α, indicating the existence of an optimum point of α for maximizing the secrecy throughput performance.

Fig. 8 plots the secrecy throughput of the SWIPT and FD self-jamming system for various α. The optimum value of α under the given parameters is α^*=0.6188. As shown in this figure, the secrecy throughput varies with the changing of α. Obviously, the secrecy throughput is not a monotonically increasing function with α as it is generally the largest when α=0.5 comparing to α=0.2 and 0.8. Furthermore, the secrecy throughput achieves its maximum value when the optimum value of α is applied, which is in exact agreement with the result in Theorem 4. In addition, it is easy to observe that the secrecy throughput performance of the proposed SWIPT-FDSJ is much better than that of the reduced HDNSJ scheme. In particular, the secrecy throughput of the reduced HDNSJ scheme approaches to zero with the increase of γ_S. By contrast, the secrecy throughput of the proposed SWIPT-FDSJ scheme approaches to a performance floor, which again indicates the superiority of our proposed SWIPT-FDSJ scheme when compared to the reduced HDNSJ scheme.

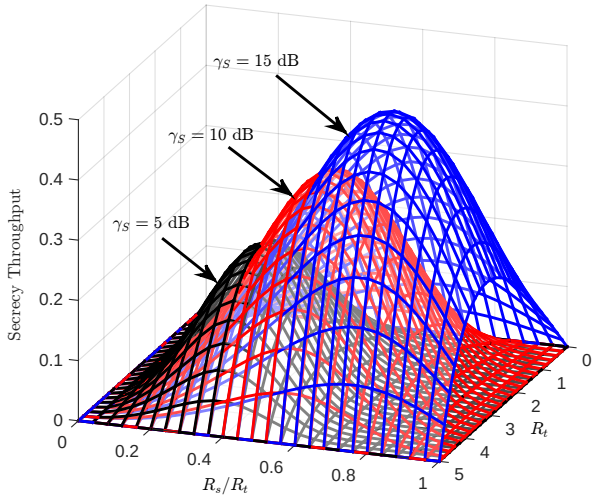


Fig. 9. Secrecy throughput vs. R_t and R_s/R_t with different γ_S. α=0.5, θ=40.

Fig. 9 plots the secrecy throughput of the SWIPT and FD self-jamming system for various R_t and R_s/R_t. It is readily to observe that for a fixed value of R_s/R_t, the secrecy throughput upgrades to its peak as R_t reaches its optimal, and then goes downwards. This phenomenon could be explained as follows. For a fixed value of R_s/R_t, increasing R_t indicates a corresponding increase of R_s, which results the increase of COP and the decrease of SOP ultimately.

When a low R_t is used, increasing COP is not distinct so that the secrecy throughput keeps increasing. However, after R_t reaches the optimal value, the secrecy throughput falls because the increase of COP becomes dominant, as it is hard for $S-D$ link to afford a reliable transmission any longer. Moreover, subject to a fixed R_t which results to a constant COP, the secrecy throughput with R_s/R_t is also a concave function, following a similar trend with R_t. We note that, the peak of secrecy throughput and the corresponding optimal point of R_s/R_t both promote as a larger γ_S is provided.

VII. Conclusions

In this paper, a new paradigm for safeguarding energy-constrained SWIPT networks was presented and the secrecy performance of the system was analyzed with the passive eavesdropping. The main idea of the scheme was that, the destination node harvested energy transmitted from the source with the MRT protocol, and then utilized it to send jamming signals to confuse the malicious eavesdropper. The exact closed-form expressions of the COP, the SOP, and the secrecy throughput were derived and their asymptotic analysis under two scenarios were carried out. Moreover, the optimal time duration allocation was conducted and the application condition as well as the maximum secrecy throughput of the proposed SWIPT-FDSJ scheme and its reduced HDNSJ scheme were provided. The results depicted that the application condition was totally determined by the system parameters, namely the transmit SNR, the antenna number of the source, the energy conversion efficiency, and the average channel gains of both the authorized and malicious links. Besides, it was proved that the secrecy throughput performance of the SWIPT-FDSJ scheme is much better than the reduced HDNSJ scheme when the application condition is satisfied.

Appendix A
Proof of Lemma 1

Without loss of generality, we define $\gamma_{SD} = P_S\|\mathbf{h}_{SD}\mathbf{w}_{SD}\|^2/N_0$, $\gamma_{JI} = P_J\left|\tilde{h}_I\right|^2/N_0$. As depicted in [49], the CDF of γ_{SD} is as follows

$$F_{\gamma_{SD}}(x) = 1 - \sum_{n=0}^{N_S-1}\frac{1}{n!}\left(\frac{N_0 x}{P_S\bar{\gamma}_{SD}}\right)^n e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SD}}}. \tag{32}$$

Obviously, the PDF of γ_{JI} can be expressed as

$$f_{\gamma_{JI}}(y) = \frac{N_0}{P_J\tilde{\bar{\gamma}}_I}e^{-\frac{N_0 y}{P_J\tilde{\bar{\gamma}}_I}}. \tag{33}$$

According to (9), we have

$$F_{\gamma_D}(x) = \int_0^\infty F_{\gamma_{SD}}(x(y+1))\, f_{\gamma_{JI}}(y)\, dy. \tag{34}$$

By applying the binomial theorem [52] in (32), we derive

$$F_{\gamma_{SD}}(x(y+1)) = 1 - \sum_{n=0}^{N_S-1}\frac{1}{n!}\left(\frac{N_0 x}{P_S\bar{\gamma}_{SD}}\right)^n e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SD}}} \times \sum_{n_1=0}^{n}\binom{n}{n_1} y^{n_1} e^{-\frac{N_0 xy}{P_S\bar{\gamma}_{SD}}}. \tag{35}$$

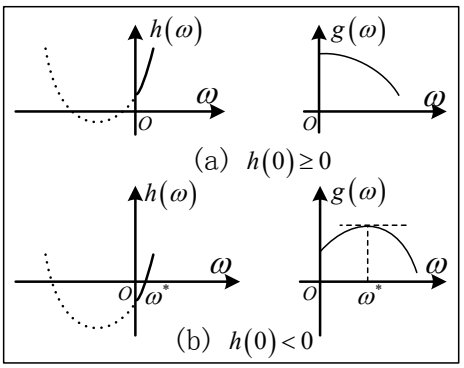


Fig. 10. $h(\omega)$ and $g(\omega)$ vs. ω with: (a) $h(0) \geq 0$; (b) $h(0) < 0$.

Substituting (33) and (35) into (34), and with the aid of [53, Eq.(3.381.4)], we obtain

$$F_{\gamma_D}(x) = 1 - \frac{N_0}{P_J\tilde{\bar{\gamma}}_I}\sum_{n=0}^{N_S-1}\frac{1}{n!}\left(\frac{N_0 x}{P_S\bar{\gamma}_{SD}}\right)^n \sum_{n_1=0}^{n}\binom{n}{n_1} \times (n_1)!\left(\frac{P_J P_S\bar{\gamma}_{SD}\tilde{\bar{\gamma}}_I}{P_J\tilde{\bar{\gamma}}_I N_0 x + P_S\bar{\gamma}_{SD}N_0}\right)^{n_1+1} e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SD}}}. \tag{36}$$

Replacing x with γ_{th}^t, and recalling (8) yields the result in Lemma 1.

Appendix B
Proof of Lemma 2

For the notation convenience, we denote $\gamma_{SE} = P_S\|\mathbf{h}_{SE}\mathbf{w}_{SD}\|^2/N_0$, $\gamma_{JE} = P_J|h_{DE}|^2$. As depicted in [54, 55] and the proof of Theorem 1, γ_{SE} is an exponentially distributed random variable and the CDF of which can be written as

$$F_{\gamma_{SE}}(x) = 1 - e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SE}}}. \tag{37}$$

In addition, the PDF of γ_{JE} is readily to be given by

$$f_{\gamma_{JE}}(y) = \frac{N_0}{P_J\bar{\gamma}_{DE}}e^{-\frac{N_0 y}{P_J\bar{\gamma}_{DE}}}. \tag{38}$$

Hence, the CDF of γ_E can be calculated as

$$F_{\gamma_E}(x) = \int_0^x F_{\gamma_{SE}}(x(y+1))\, f_{\gamma_{JE}}(y)\, dy. \tag{39}$$

Substituting (37) and (38) into (39), and after some simple manipulations, the CDF of γ_E is obtained as

$$F_{\gamma_E}(x) = 1 - \frac{P_S\bar{\gamma}_{SE}}{P_S\bar{\gamma}_{SE} + P_J\bar{\gamma}_{DE}x}e^{-\frac{N_0 x}{P_S\bar{\gamma}_{SE}}}. \tag{40}$$

Substituting (8) and (40) into (11) easily leads to the result in Lemma 2.

APPENDIX C
PROOF OF THEOREM 4

For the better explanation, we denote

$$g(\omega) = \frac{1}{1+\omega}\left(1 - \frac{\kappa_1\kappa_2}{\omega+\kappa_1}\right). \quad (41)$$

By taking the derivative of above equation, we obtain

$$\frac{dg(\omega)}{d\omega} = -\frac{h(\omega)}{(1+\omega)^2(\omega+\kappa_1)^2}, \quad (42)$$

where

$$h(\omega) = [\omega + \kappa_1(1-\kappa_2)]^2 + \kappa_1\kappa_2(\kappa_1 - 1 - \kappa_1\kappa_2). \quad (43)$$

As we see, $h(\omega)$ is a quadratic function. Also, it is readily observed that $\kappa_1 > 0$ and $1-\kappa_2 > 0$. Thereby, it is the value of $h(0)$ that solely determines the trend of $g(\omega)$. For a better comprehension, we plot the diagrams of $h(\omega)$ and $g(\omega)$ versus ω in Fig. 10 under different cases of $h(0) \geq 0$ and $h(0) < 0$.

We note, $h(0) < 0$ yields

$$\kappa_2 > \frac{\kappa_1}{1+\kappa_1}, \quad (44)$$

and when $\kappa_2 > \kappa_1/(1+\kappa_1)$, $\frac{dg(\omega)}{d\omega} = 0$ yields

$$\omega^* = -\kappa_1(1-\kappa_2) + \sqrt{\kappa_1\kappa_2(1+\kappa_1\kappa_2-\kappa_1)}. \quad (45)$$

Based on the above analysis, the results in Theorem 4 could be readily derived.

REFERENCES

[1] C. C. Y. Poon, Y. T. Zhang, and S. D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73-81, Apr., 2006.

[2] J. F. Valenzuela-Valdes, M. A. Lopez, P. Padilla, J. L. Padilla, and J. Minguillon, "Human neuro-activity for securing body area networks: Application of brain-computer interfaces to people-centric Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 62-67, Feb., 2017.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. J.*, vol. 28, no. 4, pp. 656-715, Oct., 1949.

[4] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct., 1975.

[5] H. M. Wang, C. Wang, T. X. Zheng, and T. Q. S. Quek, "Impact of artificial noise on cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7390-7404, Nov., 2016.

[6] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the secure spectral-energy efficiency tradeoff in random cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2706-2722, Oct., 2016.

[7] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128-1138, Jun., 2016.

[8] B. He, Y. She, and V. K. N. Lau, "Artificial noise injection for securing single-antenna systems," *IEEE Trans. Veh. Techno.*, vol. 66, no. 10, pp. 9577-9581, Oct., 2017.

[9] X. Chen, C. Zhong, C. Yuen, and H. H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 40-46, Dec., 2015.

[10] X. Chen, J. Chen, H. Zhang, Y. Zhang, and C. Yuen, "On secrecy performance of multiantenna-jammer-aided secure communications with imperfect CSI," *IEEE Trans. Veh. Techno.*, vol. 65, no. 10, pp. 8014-8024, Oct., 2016.

[11] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Techno.*, vol. 65, no. 4, pp. 2170-2181, Apr., 2016.

[12] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems," *IEEE Trans. Veh. Techno.*, vol. 67, no. 3, pp. 2035-2048, Mar., 2018.

[13] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135-5146, Sep., 2015.

[14] J. Zhang, C. Yuen, C. K. Wen, S. Jin, K. K. Wong, and H. Zhu, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, Jan., 2016.

[15] J. Zheng, Y. Cai, X. Shen, Z. Zheng, and W. Yang, "Green energy optimization in energy harvesting wireless sensor networks," *IEEE Commun. Mag.*, vol. 53, no. 11, pp. 150-157, Nov., 2015.

[16] W. Liu, X. Zhou, S. Durrani, H. Mehrpouyan, and S. D. Blostein, "Energy harvesting wireless sensor networks: Delay analysis considering energy costs of sensing and transmission," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4635-4650, Jul., 2016.

[17] H. Mosavat-Jahromi, B. Maham, and T. A. Tsiftsis, "Maximizing spectral efficiency for energy harvesting-aware WBAN," *IEEE J. Biomed. Health Inf.*, vol. 21, no. 3, pp. 732-742, May, 2017.

[18] Z. Ling, F. Hu, L. Wang, J. Yu, and X. Liu, "Point-to-point wireless information and power transfer in WBAN with energy harvesting," *IEEE Access*, vol. 5, pp. 8620-8628, Apr., 2017.

[19] G. Pan, H. Lei, Y. Deng, L. Fan, J. Yang, Y. Chen, and Z. Ding, "On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3831-3843, Sep., 2016.

[20] X. Chen, C. Yuen, and Z. Zhang, "Wireless energy and information transfer tradeoff for limited-feedback multiantenna systems with energy beamforming," *IEEE Trans. Veh. Techno.*, vol. 63, no. 1, pp. 407-412, Jan., 2014.

[21] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754-4767, Nov., 2013.

[22] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447-3461, Oct., 2014.

[23] Y. Zeng, and R. Zhang, "Full-duplex wireless-powered relay with self-energy recycling," *IEEE Wireless Commun. Lett.*, vol. 4, no. 2, pp. 201-204, Apr., 2015.

[24] X. Zhou, "Training-based SWIPT: Optimal power splitting at the receiver," *IEEE Trans. Veh. Techno.*, vol. 64, no. 9, pp. 4377-4382, Sep., 2015.

[25] D. Wang, R. Zhang, X. Cheng, and L. Yang, "Capacity-enhancing full-duplex relay networks based on power splitting (PS-)SWIPT," *IEEE Trans. Veh. Techno.*, vol. 66, no. 6, pp. 5445-5450, Jun., 2017.

[26] G. Pan, C. Tang, T. Li, and Y. Chen, "Secrecy performance analysis for SIMO simultaneous wireless information and power transfer systems," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3423-3433, Sep., 2015.

[27] R. Feng, Q. Li, Q. Zhang, and J. Qin, "Robust secure transmission in MISO simultaneous wireless information and power transfer system," *IEEE Trans. Veh. Techno.*, vol. 64, no. 1, pp. 400-405, Jan., 2015.

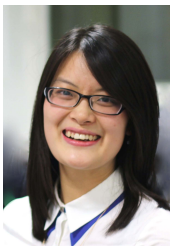
[28] W. Wu, and B. Wang, "Efficient transmission solutions for MIMO wiretap channels with SWIPT," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1548-1551, Sep., 2015.

[29] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng,

and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 104-110, Nov., 2014.
[30] H. Xing, K. K. Wong, Z. Chu, and A. Nallanathan, "To harvest and jam: A paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process.*, vol. 63, no. 24, pp. 6616-6631, Dec., 2015.
[31] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128-137, May, 2015.
[32] M. Liu, and Y. Liu, "Power allocation for secure SWIPT systems with wireless-powered cooperative jamming," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1353-1356, Jun., 2017.
[33] X. Tang, W. Yang, Y. Cai, W. Yang, and Y. Huang, "Security of full-duplex jamming swipt system with multiple non-colluding eavesdroppers," in *Proc. 2017 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Shenzhen, China, pp. 66-69, 21 Jul., 2017.
[34] W. Yang, W. Mou, X. Xu, W. Yang, and Y. Cai, "Energy efficiency analysis and enhancement for secure transmission in swipt systems exploiting full duplex techniques," *IET Commun.*, vol. 10, no. 14, pp. 1712-1720, May, 2016.
[35] J. Zhang, G. Pan, and H. M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887-3893, Jul., 2016.
[36] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447-3461, Oct., 2014.
[37] J. Zhang, G. Pan, and H. M. Wang, "On physical-layer security in underlay cognitive radio networks with full-duplex wireless-powered secondary system," *IEEE Access*, vol. 4, pp. 3887-3893, Jul., 2016.
[38] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025-3038, Jul., 2016.
[39] D. Lee, and Y. Noh, "SER analysis of scheduled TAS with MRC in the presence of non-identical channel estimation errors," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2298-2301, Dec., 2015.
[40] M. Li, M. Lin, W. P. Zhu, Y. Huang, A. Nallanathan, and Q. Yu, "Performance analysis of MIMO MRC systems with feedback delay and channel estimation error," *IEEE Trans. Veh. Techno.*, vol. 65, no. 2, pp. 707-717, Feb., 2016.
[41] Y. Ma, and J. Jin, "Effect of channel estimation errors on M-QAM with MRC and EGC in Nakagami fading channels," *IEEE Trans. Veh. Techno.*, vol. 56, no. 3, pp. 1239-1250, May, 2007.
[42] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure full-duplex spectrum-sharing wiretap networks with different antenna reception schemes," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 335-346, Jan., 2017.
[43] H. A. Suraweera, P. J. Smith, and M. Shafi, "Capacity limits and performance analysis of cognitive radio with imperfect channel knowledge," *IEEE Trans. Veh. Techno.*, vol. 59, no. 4, pp. 1811-1822, May, 2010.
[44] G. Zhu, C. Zhong, H. A. Suraweera, Z. Zhang, C. Yuen, and R. Yin, "Ergodic capacity comparison of different relay precoding schemes in dual-hop AF systems with co-channel interference," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2314-2328, Jul., 2014.
[45] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574-583, Mar., 2015.
[46] Z. Chu, T. A. Le, H. X. Nguyen, M. Karamanoglu, Z. Zhu, A. Nallanathan, E. Ever, and A. Yazici, "Robust design for MISO SWIPT system with artificial noise and cooperative jamming," in *2017 IEEE Global Communications Conference (GLOBECOM 2017)*, Singapore, pp. 1-6, 4 Dec., 2017.
[47] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. L. Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Techno.*, vol. 64, no. 5, pp. 1833-1847, May, 2015.
[48] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622-3636, Jul., 2013.
[49] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771-1783, May, 2015.
[50] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377-6388, Nov., 2015.
[51] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Techno.*, vol. 65, no. 8, pp. 6259-6274, Aug., 2016.
[52] D. W. Bolton, "The multinomial theorem," *The Mathematical Gazette*, vol. 52, no. 382, pp. 336-342, Dec., 1968.
[53] I. S. Gradshteyn, and I. M. Ryzhik, *Table of integrals, series, and products*, 7 ed., San Diego, CA, USA: Academic, 2007.
[54] M. Maleki, and H. R. Bahrami, "On the distribution of norm of vector projection and rejection of two complex normal random vectors," *Mathematical Problems in Engineering*, vol. 2015, no. 8, 2015, Art. no. 159231.
[55] M. Chraiti, A. Ghrayeb, and C. Assi, "Achieving full secure degrees-of-freedom for the MISO wiretap channel with an unknown eavesdropper," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7066-7079, Nov., 2017.
[56] C. Jian, and A. U. H. Sheikh, "Outage probability of cellular radio systems using maximal ratio combining in the presence of multiple interferers," *IEEE Trans. Commun.*, vol. 47, no. 8, pp. 1121-1124, Aug., 1999.

Xuanxuan Tang received his B.S. degree in Communication Engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2014. He is currently pursuing toward the Ph.D. degree in Information and Communications Engineering at the College of Communications Engineering, Army Engineering University of PLA, Nanjing, China. His current research interest includes cooperative communications, wireless sensor networks, Internet of Things, physical layer security, energy harvesting, full-duplex, and cognitive radio systems.

Yueming Cai (M'05-SM'12) received his B.S. degree in Physics from Xiamen University, Xiamen, China in 1982, the M.S. degree in Micro-electronics Engineering and the Ph.D. degree in Communications and Information Systems both from Southeast University, Nanjing, China in 1988 and 1996, respectively. His current research interests include MIMO systems, OFDM systems, signal processing in communications, cooperative communications and wireless sensor networks.



Yansha Deng (S'13-M'17) is currently a Lecturer (Assistant Professor) in department of Informatics, King's College London, U. K. She received the Ph.D. degree in Electrical Engineering from the Queen Mary University of London, UK in 2015. From 2015 to 2017, she was a Post-Doctoral Research Fellow with King's College London, UK. Her research interests include molecular communication, internet of things, and 5G wireless networks. She was a recipient of the Best Paper Awards from ICC 2016 and Globecom 2017. She is currently an Editor of IEEE Transactions on Communications and IEEE Communication Letters. She has also served as TPC member for many IEEE conferences, such as IEEE GLOBECOM and ICC.

Yuzhen Huang (S'12-M'16) received his B.S. degree in Communications Engineering, and Ph.D. degree in Communications and Information Systems from College of Communications Engineering, PLA University of Science and Technology, in 2008 and 2013, respectively. Now, he has been with the Artificial Intelligence Research Center, National Innovation Institute of Defense Technology, and currently as an Research Associate. He also is a Post-Doctoral Research Associate with the School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing. His research interests focus on channel coding, MIMO communications systems, cooperative communications, physical layer security, and cognitive radio systems. He has published nearly 70 research papers in international journals and conferences. He and his coauthors have been awarded a Best Paper Award at the WCSP 2013. He received an IEEE Communications Letters exemplary reviewer certificate for 2014.

Wendong Yang received the B.S. degree in Communications Engineering and the Ph.D. degree in Communications and Information Systems both from College of Communications Engineering, PLA University of Science and Technology, Nanjing, China in 2004 and 2009 respectively. His current research interest includes MIMO systems, OFDM systems, cooperative communications and cognitive radio.

Weiwei Yang (S'08-M'11) obtained his B.Sc. degree, M.Sc. degree, and Ph.D. degree in Telecommunications from PLA University of Science and Technology, Nanjing, China in 2003, 2006, and 2011, respectively. Currently he is an Associate Professor in College of Communication Engineering,Army Engineering University of PLA. His research interests include cooperative communications, cognitive radio, and physical layer security. He is also co-recipient of Best Paper Award from WCSP 2011. He also served as a publication Co-Chair of WCSP 2015, track chairs of IEEE CIC ICCC 2017 and WCSP 2015,and TPC members of WCSP 2011/2014/2017,GC 2016 Workshops, GC 2017 Workshops and ICC 2016-Workshops, etc. He is a co-author of the book"Handbook of Cognitive Radio" published by Springer in 2017.